Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.15.x

First Published: 2024-08-27

Last Modified: 2026-10-01

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.

- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Manager Release 20.15.1

These release notes accompany the Cisco Catalyst SD-WAN Control Components, Release 20.15.x, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager as applicable to Cisco Catalyst SD-WAN.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE Catalyst SD-WAN device, Cisco IOS XE Release 17.15.x.

What's New for Cisco Catalyst SD-WAN Manager Release 20.15.1

Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides.

Table 1: Cisco Catalyst SD-WAN Manager Release 20.15.1

Feature	Description
Cisco Catalyst SD-WAN Monitor and Maintain	
Converged Cisco SD-WAN Manager and Cisco SD-WAN Analytics Dashboard	This feature introduces a converged dashboard in Cisco SD-WAN Manager that merges the monitoring and analytics capabilities from both Cisco SD-WAN Manager and Cisco SD-WAN Analytics. This converged dashboard displays management data from the Cisco SD-WAN Manager alongside analytical insights from Cisco SD-WAN Analytics, all within a single interface. To view a converged dashboard in Cisco SD-WAN Manager, Cisco SD-WAN Analytics must be onboarded into Cisco SD-WAN Manager.
Additional Report Types and Formats	This feature introduces several new report types, including Security reports, which are available in CSV or PDF format.
Additional Report Filters and Download Options	Generate new report types and download them in both PDF and CSV formats. The **My Reports** and the **Generate** report forms are updated to include additional report filters.

Feature	Description
Generate an Admin-Tech File with Custom Commands	This feature enhances the output of the admin-tech file with additional command output information. With this feature, You can generate a customized admin-tech file with the required show command output details to help in troubleshooting. Custom admin-tech is independent of tech, core, and logs flag.
Cisco Catalyst SD-WAN Security	
Share Traffic Information with Cisco Security Service Edge	Cisco SD-WAN Manager shares VPN and security group tag (SGT) information with Cisco Security Service Edge (SSE). This is called context information. SSE applies different policies to traffic based on the context information of the traffic.
Cisco Catalyst SD-WAN Systems and Interfaces	
Configure EtherChannels using Configuration Groups	With this feature you can configure EtherChannels on service and transport side using configuration groups.
Load Balancing for EtherChannels on Individual Port Channels	With this feature you can load balance EtherChannels for individual port channels on service and transport side using CLI templates.

Table 2: Cisco Catalyst SD-WAN Manager Release 20.15.2

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
RSA Key Length Increase in Cisco SD-WAN Manager	Introduces 4096-bit RSA key support for certificate signing requests (CSR) for enterprise certificates.
Cisco Catalyst SD-WAN Policy Groups	
Enhancements to Security Policy Using Policy Groups	The following enhancements are introduced with this release: • **Embedded Security** is called **NGFW** in Cisco SD-WAN Manager. • Create copies of security policy and sub-policy. • View all configured rules for specific policies in the **NGFW** policy dashboard. • For each rule, **Clone rule**, **Add rule on top**, and **Add rule below** options are added.

Table 3: Cisco Catalyst SD-WAN Manager Release 20.15.3

Feature	Description
Cisco Catalyst SD-WAN Configuration Groups	

Feature	Description
Cisco Secure Platforms support with configuration groups	From Cisco Catalyst SD-WAN Manager Release 20.15.3, these Cisco Secure Platforms are introduced and can only be configured using configuration groups. • C8375-E-G2 • C8570-G2 • C8550-G2 • C8475-G2 • C8455-G2

Table 4: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Feature	Description
Cisco Catalyst SD-WAN Systems and Interfaces	
Layer 2 (L2) VPN Multihoming and Hub-and-Spoke Support	With this feature, you can configure Layer 2 VPN on multiple devices on the same site in an active/standby configuration. This feature also enables Layer 2 connections using an indirect path, such as a hub, for point-to-multipoint connections within the Cisco Catalyst SD-WAN fabric.
Configure EtherChannels using Configuration Groups	With this feature you can configure EtherChannels on service and transport side using configuration groups.
Load Balancing for EtherChannels on Individual Port Channels	With this feature you can load balance EtherChannels for individual port channels on service and transport side using CLI templates.
Cisco Catalyst SD-WAN Routing	
BFD Troubleshooting for Cisco Catalyst SD-WAN Using Radioactive Tracing	This feature provides the ability to troubleshoot BFD protocols using radioactive (RA) tracing. RA tracing enables debug logs across various processes which participates and handles a particular BFD session.
Multicast Support for Hub and Spoke Topologies	This feature enables efficient distribution of one-to-many traffic for hub and spoke devices. The multicast routing protocols like, IPv4 Multicast, IGMPv3, PIM SSM, PIM ASM, Auto RP and Static RP distribute data to multiple recipients. Using multicast overlay protocols in hub and spoke topology, a source can send a single packet of data to a single multicast address, which is then distributed to an entire group of recipients.
Cisco Catalyst SD-WAN Policies	

Feature	Description
Packet Duplication using Underlay Fragmentation	This feature uses adjacency MTU to combine with underlay fragmentation which allows the successful transmission of packets that exceed the MTU limitations by breaking them down into manageable fragments and ensuring their reliable delivery.
Remote Preferred Color in Data Policy	You can set a remote preferred color in the data policy to control traffic routing based on the SLA criteria. See for Configure Traffic Rules information.
Service Insertion for Equinix	With this feature, you can deploy Palo Alto Networks firewall on Equinix and attach a service chain to Equinix interconnect gateway from the **Workflow Library** in Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Security	
Cisco Umbrella Scope Credentials	This feature provides the ability to define and configure a new single Cisco Umbrella credential for both Umbrella SIG and Umbrella DNS.
Enhanced SGACL Logging	This feature enhances the Security Group Access Control List (SGACL) logging capability by using High Speed Logging (HSL) for Cisco IOS XE Catalyst SD-WAN devices. SGACL logging through HSL provides a logging method for security events that is more efficient and capable of scaling, useful in network environments experiencing high volumes of traffic.
Zscaler Sub-locations	This feature supports configuration of one or more Zscaler sub-locations for a given location.
Cisco Catalyst SD-WAN Firewall High Availability	By implementing High Availability (HA) in Cisco Catalyst SD-WAN, you can set up two Cisco IOS XE Catalyst SD-WAN devices in either active-active or active-standby configurations. When HA is enabled, features like the Zone Based Firewall (ZBF) and Network Address Translation (NAT) utilize this functionality to synchronize their states between the devices, whether in active-standby or active-active modes. In the event of a failure of the active device, the standby device seamlessly takes over operations without interrupting session flows, thus eliminating the need for reconnection.
Share Traffic Information with Cisco Security Service Edge	Cisco SD-WAN Manager shares VPN and security group tag (SGT) information with Cisco Security Service Edge (SSE). This is called context information. SSE applies different policies to traffic based on the context information of the traffic.
Cisco Catalyst SD-WAN Cloud OnRamp	
Cloud OnRamp for SaaS Workflow	Cisco SD-WAN Manager allows you to select specific SaaS applications and identify best performing paths for each of these SaaS applications using a fully-guided workflow.
Cisco Catalyst SD-WAN Monitor and Maintain	
Alarm Notifications Using WebHooks	Configure a WebHook URL in Cisco SD-WAN Manager to receive alarm notifications in Webex or Slack.

Feature	Description
Connect to and troubleshoot Cisco Catalyst SD-WAN solution using Cisco RADKit	Use tools and Python modules from Cisco Remote Automation Development Kit (RADKit) to securely connect to remote terminals, WebUIs, or desktops. Using RADKit, a TAC engineer can request the required information during the troubleshooting process, from the various devices and services, in a secure and controlled way.
Generate an Admin-Tech File with Custom Commands	This feature enhances the output of the admin-tech file with additional command output information. With this feature, You can generate a customized admin-tech file with the required show command output details to help in troubleshooting. Custom admin-tech is independent of tech, core, and logs flag.
View Packet Duplication Information for Tunnels	This feature provides a single chart option in Cisco SD-WAN Manager for viewing packet duplication information for tunnels.
Cisco Catalyst SD-WAN NAT	
Application-Level Gateway (ALG) in Service-Side NAT	Use an application-level gateway (ALG) to interpret the application-layer protocol and perform service-side NAT translations for FTP protocol.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	
Create Regions and Assign Controllers Workflow	Cisco SD-WAN Manager introduces a fully-guided workflow that allows you to create multiple regions within your Cisco Catalyst SD-WAN fabric and assign Cisco SD-WAN Controllers to them.
Policy Groups	
Preferred Remote Color in AAR Policy	You can set a remote preferred color in the AAR policy to control traffic routing based on the SLA criteria.
Region Support for Topology	**Level** topology attribute is supported for custom topologies where you could choose between **Sites** and **Regions**. When you add rules to your topology, match conditions using the **Region** condition.
Regions Support for Policy Groups	Associate devices from a particular region or subregion while deploying policy groups.
Cisco Catalyst SD-WAN Configuration Groups	
Configuration Catalog	This feature introduces a catalog functionality which provides a collection of pre-defined intent based configurations and policies. The Cisco Catalyst SD-WAN Portal hosts the catalog service, which is managed by Cisco. The Cisco SD-WAN Manager can download the readily available, cloud-hosted catalog entries from the Cisco Catalyst SD-WAN Portal and customize them as needed before deploying the configuration objects from the catalog entry onto devices in their network.

Feature	Description
Create a Configuration Group Without Using a Workflow	This feature introduces a method for creating configuration groups directly on the **Configuration Groups** page of Cisco SD-WAN Manager without launching a workflow. After selecting a product solution, you can create a configuration group based on the available profiles for that solution. Cisco SD-WAN Manager creates the configuration group with the required profiles, which you can configure based on your requirement. This feature allows you to reuse previously created profiles. You can create, manage, and deploy the configuration group from one page.
Support for Specifying Default Values for Device Specific Variables of a Feature	You can provide a default value along with description to feature parameters when you select the **Device Specific** scope. Cisco SD-WAN Manager applies the default value of the parameter to the device while deploying the configuration group.
Cisco Catalyst SD-WAN Network-Wide Path Insight User	
Visibility into IPsec Drops	This feature provides enhancements to the Network-Wide Path Insight feature to provide granular visibility into the IPsec drops.
Cisco Managed Cellular Activation	
Managed Cellular Activation support for the IoT platforms and modules	The Managed Cellular Activation solution is supported in the IoT platforms and modules.
Cisco Catalyst SD-WAN Rugged Series Router Configuration Guide	
Configure GNSS on PIMs Using Cisco SD-WAN Manager	This feature allows you to configure and manage the GNSS (Global Navigation Satellite System) PIM module on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager.
Deploying Smart Licensing Using Policy in Cisco Catalyst SD-WAN	
Workflow for Assigning Licenses to Devices	Introduced the License Assignment Workflow for assigning licenses to devices.
Cisco Catalyst SD-WAN Integrations	
Cisco Cyber Vision Integration	Cisco SD-WAN Manager supports integration with the Cisco Cyber Vision network security solution. You can configure devices in the network to monitor and inspect traffic on one or more interfaces and send traffic metadata or a copy of your network traffic to Cisco Cyber Vision Center to analyze it for security concerns.

Table 5: Cloud-delivered Cisco Catalyst SD-WAN

Field	Description
Interconnect Between Cisco Catalyst SD-WAN and Cisco Meraki SD-WAN	Cisco SD-WAN Interconnects is an automated workflow which enables administrators to easily configure, deploy, and monitor an interconnect between Cisco Catalyst SD-WAN and Cisco Meraki SD-WAN topologies using the Cisco Meraki dashboard. You can monitor IPsec tunnel status, eBGP session status, and VPN tunnel statistics from the Interconnects page on the Cisco Meraki dashboard.

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Manager Release 20.15.x

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Control Components Release 20.15.5

Behavior Change	Description
Cloud gateway exemption from license requirement: No license is required for up to two Cisco 8000V devices if: • They are operating as cloud gateway routers for a Cisco SD-WAN Cloud Pro environment (Cisco cloud-hosted), and • They provide a gateway for a TACACS or syslog server located outside the Catalyst SD-WAN fabric. The license exemption requires tagging the devices with the Connector tag. After tagging the devices, the license compliance check will not flag them as requiring a license, and SD-WAN Manager will not show an out-of-compliance message for the devices.	

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Control Components Release 20.15.2

Behavior Change	Description
Routes that are re-originated from a site through the transport gateway are filtered out by the Cisco Catalyst SD-WAN Controller. These re-originated routes are not sent back to the originating site or the sites which share same site ID as the originating site. The re-originated routes are only distributed to different sites within the Cisco Catalyst SD-WAN network.	See the Re-originating Routes section.

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Control Components Release 20.15.1

Behavior Change	Description
When configuring a configuration group for Cisco IOS XE Catalyst SD-WAN devices, to configure cellular connectivity, you can add a Cellular Profile. To add a Cellular Profile, open the Transport & Management Profile, add a Cellular Controller feature, then add a Cellular Profile as a child feature of Cellular Controller. The Cellular Profile includes fields for the authentication credentials to connect to a cellular network. When you enter a password in the Profile Password field, Cisco SD-WAN Manager encrypts the password. When you display the CLI commands that make up a device configuration in the configuration preview, Cisco SD-WAN Manager displays the password in its encrypted form, not as plain text.	Refer to the Cellular Profile section.
There is a default RBAC role called security_operations. In Cisco Catalyst SD-WAN Manager Release 20.13.x and 20.14.x, this role included permission to enable or disable Cloud SaaS feeds. In Cisco Catalyst SD-WAN Manager Release 20.15.x, the security_operations role no longer has this permission.	Refer to the Restrictions for Role Based Access Control section.
Updated the **aaa netconf-accounting** command with supported options.	Refer to the aaa netconf-accounting command.

Behavior Change	Description
Unsupported SHA-1 authentication	From Cisco Catalyst SD-WAN Control Components Release 20.15.1, the SHA-1 authentication algorithm is not supported. If an SNMPv3 user is configured with SHA-1 authentication, the upgrade to Release 20.15.1 or later fails and displays an error indicating the use of deprecated security configurations. To proceed with the upgrade, you must complete one of the following actions either before or during the upgrade: • **Delete** the SNMPv3 user configured with SHA-1, or • **Reconfigure** the SNMPv3 user to use a supported authentication algorithm (such as SHA-256). For more information, refer to SNMP Configuration Guide
The `attachfeature` API now requires the `isEdited` and `isMasterEdited` flags to be set to 'True' as appropriate when attaching a Device Template. Set `isMasterEdited` to 'True' for Master Template edits and `isEdited` to 'True' for Feature Template edits to ensure changes are correctly applied.	For more information, refer to Feature Template
Perpetual licenses From Cisco Catalyst SD-WAN Control Components Release 20.15.1, Catalyst SD-WAN does not support perpetual licenses, except for High Security (HSEC) licenses. It supports term-based licenses.	For more information, refer to Deploying Smart Licensing Using Policy in Cisco Catalyst SD-WAN.
When configuring an ethernet interface, using a configuration group, if you enter a variable in the **IP Address** field, the **Subnet Mask** field automatically uses a variable also.	Refer to Ethernet Interface.
Supported Characters in Variable Values	Semicolons (;) are not supported in variable values. To separate multiple CLI lines, use the newline character (\n) instead.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Table 6: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Behavior Change	Description
Updated the **show platform software ipsec fp active flow** command output.	The output of the **show platform software ipsec fp active flow** has been modified. The flow ID now supports a range between 0 - 4294967295. See the show platform software ipsec fp active flow command.
Updated the SLA class threshold values.	See the SLA Classes section, which describes the new SLA class threshold values.
Updated the **request platform software sdwanadmin-tech** command with supported options.	See the request platform software sdwan admin-tech command.
Updated the Policy Object Profile section with the new behavior on pagination when there are more than 50 profiles.	See the Policy Object Profile section.
Updated the size limit of the organization name to the range 1 to 128 for the organization-name command and the size limit of the interface name to the range 1 to 31 for the interface command.	See the sp-organization-name (system) and interface sections.
Updated the Configure Device Values section with the change in configuration groups for rollback timer. Only the Cellular Gateway solution in the configuration groups supports the rollback timer.	See the Configure Device Values section.
Updated the View Cflowd Information section for the show sdwan app-fwd cflowd commands to include support for up to 4000 flow records for each monitor (IPv4 and IPv6) from the cflowd database.	See the View Cflowd Information section.
Updated the Configure BFD for Routing Protocols section to include that the BFDs on the tunnel interface are inactive if sdwan mode is not configured for the tunnel interface.	See the Configure BFD for Routing Protocols section.
Information about provider and tenant remote servers and images on Cisco SD-WAN Manager.	See the Provider and Tenant Remote Servers and Images section.
Configuration of devices in SDCI cloud gateway extension using configuration groups is not supported.	See the Information About Configuring Devices for AWS Integration Using Configuration Groups section.
The policer increases the burst value when the user-configured value is lower than the calculated value, to prevent congestion and ensure optimal performance.	See the Policer Burst Tolerance section.

Behavior Change	Description
A static IP address is assigned by default if you assign a private color to a WAN interface while configuring a site using the configuration group workflow.	See the Overview of Configuration Group Workflows section.
Updated the **Response Code End** field in the Hunt Stop Rules table for consistency.	See the Server Group section.
In Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and earlier, click the **Send to Validator** button to send only the controller's serial number once to the Cisco Catalyst SD-WAN Validator.	See the Send the Controller Serial Numbers to Cisco Catalyst SD-WAN Validator section.

Important Notes, Known Behaviors, and Workarounds

Multi-Region Fabric

Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Cisco Catalyst SD-WAN Control Components Release 20.15.x are the last releases to support these features:

- Secondary regions
- Subregions
- Management regions

From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1, configuration of these features is possible only by API.

Because later releases do not support these features, we advise you to update your network design and configuration to use alternative solutions where possible.

See End of support for three types of regions for further details.

Upgrade to 20.15.5

Upgrading from Cisco Catalyst SD-WAN Control Components Release 20.15.x to 20.15.5 causes loss of custom widgets (custom panes, or dashlets) on the SD-WAN Manager dashboard. This occurs only if Analytics is also enabled. There is no known workaround, so it requires re-adding the widgets. This includes upgrades...

from:

20.15.1 through 20.15.4

to:

20.15.5

Upgrading from 20.15.5 to later 20.15.x releases does not create this problem.

IPsec tunnel mode command removed after configuration group deployment

In SD-WAN Manager versions 20.15.4.2 and 20.15.4.4, deploying a non-CLI configuration group that includes an IPsec feature can remove the **tunnel mode ipsec ipv4** command from the Cisco IOS XE Catalyst SD-WAN device configuration.

Workaround: Add the following configuration to the device using a CLI Add-on template:

```
interface TunnelXYZ
          tunnel mode ipsec ipv4
          tunnel mode ipsec ipv4-old
```

Replace TunnelXYZ with the applicable tunnel interface name.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.x

This section details all fixed and open bugs for this release. These are available in the Cisco Bug Search Tool through the Resolved Bug Search.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.6.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.6.1

Identifier	Headline
CSCww79570	Cisco Catalyst SD-WAN Manager API authentication bypass vulnerability.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.6.1

There are no customer impacting bugs that were identified in this release.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.6

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.6

Identifier	Headline
CSCwp11066	High-volume event queries cause the Cisco Catalyst SD-WAN Manager database to exhaust memory, which forces the controller to restart.
CSCwu65699	Overlapping PAM authentication attempts cause the "aaad" daemon on the Cisco Catalyst SD-WAN Manager to crash unexpectedly.
CSCwo09151	The Centralized policy incorrectly restricts commented-out CLI commands.
CSCws83671	Following the MT cluster upgrade from 20.15.306 to 20.15.403, the Cisco Catalyst SD-WAN Manager and the Cisco Catalyst SD-WAN Validator lose device serial numbers.
CSCws99393	Navigating the topology page causes the Inbound and Outbound site entries to disappear.
CSCwo96247	Users cannot clear a stuck Configuration Group task on the Cisco Catalyst SD-WAN Manager via an API call

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.6

Identifier	Headline
CSCwv80117	Software edge devices renew certificates signed by the Cisco Catalyst SD-WAN Manager.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5.3

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5.3

Identifier	Headline
CSCwu18563	Cisco Catalyst SD-WAN Controller authenticated privilege escalation vulnerability.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5.3

There are no customer impacting bugs that were identified in this release.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5.2

Identifier	Headline
CSCwt50498	Cisco Catalyst SD-WAN Controller authentication bypass vulnerability.
CSCwt38739	Cisco Catalyst SD-WAN Manager privilege escalation vulnerability.
CSCwt55544	Cisco Catalyst SD-WAN Manager XML external entity injection vulnerability.
CSCwt38767	Cisco Catalyst SD-WAN Manager privilege escalation vulnerability.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5.2

There are no customer impacting bugs that were identified in this release.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5

Identifier	Headline
CSCwq48395	SDWAN Controller retains stuck exported routes after a policy change.
CSCws05853	Site List under Topology Policy under Topology Policy creation displays site IDs from other tenants.
CSCwp34690	License reporting fails to report to the CSSM server after a DR switchover in 20.18.
CSCwq28772	The preferred remote color restrict feature does not work on SD-WAN Manager 20.15.3.

Identifier	Headline
CSCwr88750	SD-WAN Manager generates the guest IP address and VirtualPortGroup IP address from different subnets.
CSCwd58323	SD-WAN Manager fixes the Azure AD SSO maxAuthenticationAge at 7200 seconds.
CSCwo52922	SD-WAN Manager database does not find the license although it is present.
CSCwn26880	Config-db does not remove commented lines from the configuration when using a CLI-based centralized policy.
CSCwn64946	An Olap-db connection leak causes the UI to stop responding and triggers a 180-second timeout.
CSCwq10559	The network hierarchy page becomes unavailable due to missing SD-WAN Controllers in the user scope.
CSCwn19192	An offline node from SD-WAN cluster is not getting removed.
CSCwq98192	vmanage high CPU utilization because of vdaemon-message processes leaking on socket 'CLOSE_WAIT'
CSCwr14063	SD-WAN Manager experiences high CPU utilization because vdaemon-message processes leak on the 'CLOSE_WAIT' socket.
CSCwq79825	The vDaemon process crashes when attempting to parse the SD-WAN Manager system IP.
CSCwp85929	Changing the sequence of rules in the centralized policy causes misprogramming on SD-WAN Controller.
CSCwq10572	Vault exits after an upgrade in the Disaster Recovery cluster in 20.18.
CSCwq37648	The UC upgrade does not work when the neo4j password contains special characters.
CSCwp38011	Support for replication of file system data as part of DR.
CSCwr71504	Task status is success despite topology configuration not being pushed to SD-WAN Controller.
CSCwp27667	The edge count does not match the tenant edge count.
CSCwq14387	The UX 2.0 configuration group loses variable values.
CSCwp83222	SD-WAN Manager does not display multiple next-hop entries for ECMP routes in the IP Route real-time table.
CSCwo62038	SD-WAN Manager SSO with Azure assigns incorrect resources or scopes for remote users.
CSCwm74306	The Switchport Parcel in the Configuration Group enables 802.1X by default.
CSCwr89351	SD-WAN Manager CPU load values reported in the WAN Edge Health and System Status sections do not match.

Identifier	Headline
CSCwk97594	SD-WAN Manager upgrade from 20.9.5.1 to 20.12.3 fails due to a neo4j authentication failure.
CSCwm61587	User cannot search for the configuration preview within the Configuration Group.
CSCws03221	There is an error installing wrong ThousandEyes image due to multiple architectures in the repository.
CSCwr79876	SD-WAN Manager removes the NAT bypass from the policy group.
CSCwq91481	Scale configuration causes neo4j to crash and restart in the secondary node when deleting and importing SYSTEMDEVICESNODE during disaster recovery.
CSCwp02968	The Tunnel Page graph may appear blank for a device in SD-WAN Manager.
CSCwq86617	Network rediscovery triggers high CPU utilization on the Neo4j leader node.
CSCwm45553	The time format changes in the API body in SD-WAN 20.14 and 20.15.
CSCwp35976	Viptela devices experience intermittent login issues when AAA accounting is enabled.
CSCwq70818	ip source-route is unexpectedly enabled after pushing a configuration group.
CSCwq58262	Despite the topology not being activated, the task status shows as success.
CSCwq33835	Disaster recovery replication fails with a large configuration, causing a Neo4j Out of Memory (OOM) error on the standby node.
CSCws05835	Topology Group creation fails with the reason "Feature Profile failed" on the first attempt.
CSCwp15172	SD-WAN Manager 20.15.x cannot SSH into vEdge cloud or SD-WAN Validator.
CSCwq65340	SD-WAN Manager 20.12.5 exhibits incorrect behavior when cancelling a change to the Centralized Policy after adding topology.
CSCwq42160	The UX 2.0 dual device configuration group loses variable values when a device is disassociated.
CSCwo45368	Manager Web CSR generation is unusable because the email address is appended to the SAN instead of the subject.
CSCwq84802	It is not possible to add more than 2000 characters in a prefix list within Configuration Groups in 20.15.3.1.
CSCwp99414	The certificate workflow cannot reach SD-WAN Validator after a Disaster recovery switchover.
CSCwn08200	The SD-AVC container status becomes unreachable after multiple enable/disable actions in Settings.
CSCwn35036	The Bulkapi state API GET returns incorrect records in 20.15.1
CSCwq29080	The configuration group policy does not display the newly created Group of Interest.

Identifier	Headline
CSCwm64271	One SD-WAN Manager in a 3-node cluster does not generate memory-usage events.
CSCwq57458	The Upgrade Coordinator reports success even when it fails to clear the MW flag.
CSCwq97540	IPv4 Route not installed after upgrade in AWS with IPv4/IPv6 Dual Stack enabled, which results in a failed upgrade.
CSCwr14030	Some SD-WAN Validators cannot connect to the new active cluster after a Disaster recovery switchover.
CSCwp65998	Rate limit value for URL non bulk api will be reset to default "100" after reboot in 20.12 / 20.15.
CSCwr96258	SD-WAN Manager syslog shows the TACACS Secret Key in plain text even when the template pushes it as encrypted.
CSCwp55823	Configuration Group variables are removed when any unassigned device is attempted to deploy and then removed.
CSCws36801	The multitenant upgrade fails due to an application-server failure.
CSCwn05753	The NGFW policy edits fails.
CSCwr28844	IDP initiated login does not work.
CSCwr33423	The Firewall High Availability Service Profile in SD-WAN imposes a static NAT entry limitation.
CSCwr92492	The quick connect workflow for Nutella (ISR1100) and CG522 does not complete.
CSCwq21361	The SD-WAN Manager GUI upgrade from 20.15.2 to 20.15.3 fails and requires a CLI upgrade.
CSCwr87014	cEdge device is missing "tunnel mode ipsec ipv4" after deploying a policy group.
CSCwq97113	SD-WAN Manager wipes daily backups from the disk on on-premise systems.
CSCwp05800	Dropping labels or nodes causes an Out of Memory (OOM) error on a scaled setup.
CSCwr13077	Imported and exported CSV files contain different values in configuration group add-on CLI variable values.
CSCwq74763	SD-WAN Manager times out while users are actively working within the application.
CSCwq84823	The device software download from the SD-WAN Manager Remote Repository fails: "Image Repository Access Check: Failed to recv file".
CSCwp27018	The BFD Summary aggregation for full BFD connectivity is incorrect because it does not consider sites with ENCS and SD-WAN devices.
CSCwm35064	Multiple SD-WAN Manager cluster nodes experience high CPU utilization randomly in 20.9.5.2.7.
CSCwq69370	SD-WAN Manager UI doesn't load due to the excessive size of Angular module files.

Identifier	Headline
CSCws02678	Tunnel statistics do not get converted to site health summary.
CSCwq15493	Group of interests get deleted, including those predefined by Cisco.
CSCwp98827	Embedded security rules fail to load due to a high number of service profiles.
CSCwq86700	The Centralized Policy page does not load in 20.12.5.
CSCwo44239	The Service Chain dropdown in Policy Configuration does not display any configured Service Chains.
CSCws32369	CLI Add-On is not getting saved for the configuration group due to an "Invalid variable" error when comments contain text.
CSCwm97086	A deleted feature parcel remains in the list view within the Configuration Group.
CSCwq80027	A new prefix list does not get created from route policy in Configuration Groups within a multitenant SD-WAN Manager setup.
CSCwq11932	A device attempts to download old UTD signature files from an SD-WAN Manager cluster node that is no longer available.
CSCwn93532	The TLOC_UP alarm is missing from SD-WAN Manager.
CSCwo59694	YANG: Unable to deploy 'aaa accounting network' command

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.5

Identifier	Headline
CSCws12781	SD-WAN Manager displays duplicate devices for custom roles.
CSCws83671	SD-WAN Manager and Validator lose device serial numbers after an multitenant cluster upgrade from 20.15.306 to 20.15.403.
CSCwj13394	SD-WAN Manager flushes active user sessions within 10 minutes of login, causing abrupt UI logouts.
CSCwh81860	The transport interface parcel with the "Auto negotiate" default fails for C8500L-8S4X platforms.
CSCwm07390	Certificate Status on SNs shows "Not Configured" even though the configuration is complete.
CSCvr12395	SD-WAN Manager pushes "media-type rj45" when attempting to configure duplex on ISR1k.
CSCwm26607	SD-WAN Manager 20.12 removes the NAT egress-interface option from the device configuration.
CSCwp97237	Enabling one IDP and disabling another causes an Internal Server Error in version 20.12.4.1.

Identifier	Headline
CSCwr85293	Hub and Spoke topology does not get deployed because it cannot find the configuration-group.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.5

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.5

Identifier	Headline
CSCwu18563	Cisco Catalyst SD-WAN Controller authenticated privilege escalation vulnerability.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.5

There are no customer impacting bugs that were identified in this release.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.4

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.4

Identifier	Headline
CSCwt50498	Cisco Catalyst SD-WAN Controller authentication bypass vulnerability.
CSCwt38739	Cisco Catalyst SD-WAN Manager privilege escalation vulnerability.
CSCwt55544	Cisco Catalyst SD-WAN Manager XML external entity injection vulnerability.
CSCwt38767	Cisco Catalyst SD-WAN Manager privilege escalation vulnerability.
CSCwu89597	Cisco IOS XE Catalyst SD-WAN device fails to retain 'tunnel mode ipsec ipv4' configuration after CLI/Add-On template deployment.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.4

There are no customer impacting bugs that were identified in this release.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.2

Identifier	Headline
CSCwp02968	SD-WAN Manager: Tunnel page graph may be blank for a device.
CSCwt15151	3 node MT cluster upgrade: statistics migration task does not kick in post upgrade.
CSCws33583	Cisco Catalyst SD-WAN Manager has an information disclosure vulnerability.
CSCws33584	Cisco Catalyst SD-WAN Manager has an arbitrary file overwrite vulnerability.

Identifier	Headline
CSCws33585	Cisco Catalyst SD-WAN Manager has an information disclosure vulnerability.
CSCws33586	Cisco Catalyst SD-WAN Manager has an arbitrary file overwrite vulnerability.
CSCws33587	Cisco Catayst SD-WAN has an authentication bypass vulnerability.
CSCws52722	Cisco Catalyst SD-WAN Controller has an authentication bypass vulnerability.
CSCws93470	Cisco Catalyst SD-WAN Manager has a privilege escalation vulnerability.
CSCwu89597	Cisco IOS XE Catalyst SD-WAN device fails to retain 'tunnel mode ipsec ipv4' configuration after CLI/Add-On template deployment.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.2

There are no customer impacting bugs that were identified in this release.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.1

Identifier	Headline
CSCwp85929	Changing the sequence of rules in a centralized policy causes misprogramming in Cisco SD-WAN Controller.
CSCwq42160	UX 2.0 loses dual device configuration group variable values when device is disassociated.
CSCwq69370	Cisco SD-WAN Manager UI fails to load due to the excessive size of Angular module files.
CSCwq74763	Cisco SD-WAN Manager times out while users are actively working in the Cisco SD-WAN Manager.
CSCwn35036	[20.15.1-459] The BulkAPI state API GET returns incorrect records.
CSCwp98827	Embedded Security Rules fail to load due to a high number of service profiles.
CSCwq70818	Cisco SD-WAN Manager enables 'ip source-route' unexpectedly after pushing a configuration group.
CSCwn64946	An olap-db connection leak causes the UI to become unresponsive and triggers a 180 second timeout.
CSCwq15493	The system deletes groups of interest, including those predefined by Cisco.
CSCwq08068	Cisco SD-WAN Manager encounters errors when applying a new Policy Group due to PSK issues on SIG tunnels.
CSCwp65998	Resetting of the rate limit value for URL non-bulk API to the default "100" after rebooting in versions 20.12/20.15.

Identifier	Headline
CSCwp55823	Cisco SD-WAN Manager removes configuration group variables when it attempts to deploy and then remove an unassigned device.
CSCwq79825	Cisco SD-WAN Manager encounters errors when applying a new Policy Group due to PSK issues on SIG tunnels caused by the restriction on the ';' character.
CSCwm45553	The time format changes in the API body in Cisco SD-WAN Manager in versions 20.14/20.15.
CSCwq11932	The Cisco IOS XE Catalyst SD-WAN device tries to download an old UTD signature file from a node of the Cisco SD-WAN Manager cluster, which is no longer available on that node.
CSCwp01581	You need to update obsolete nodes in the templates for route-map obsolete nodes.
CSCwq10572	[20.18] Vault exited after upgrade in DR Cluster

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4.1

There are no customer impacting bugs that were identified in this release.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4

Identifier	Headline
CSCwo41540	Template push for large number of devices is failing
CSCwq10572	20.18: Vault exited after upgrade in the DR Cluster.
CSCwo35654	User is unable to deploy firewall High Availability Interconnect on Sub-Interface using Cisco SD-WAN Manager
CSCwn87587	Java "Too many open files" error seen to due "analytics.sdwan.cisco.com" connection not closed
CSCwo12985	20.15 Zscaler SSE: Same location name should not allow entering the same location name for dual routers.
CSCwm96920	20.15.2 : UTD installation failing due to Error 416 after doing DR Switchover
CSCwm73117	Cisco SD-WAN Manager GUI running 20.12.4 is missing categories
CSCwp21356	Cisco SD-WAN ManagerReference Count not displaying any policies attached
CSCwo91814	Cisco SD-WAN Manager could experience high CPU with config-db during Stats/Data collection
CSCwo99367	Topology Policy is missing Match Aggregate Origin
CSCwm57287	Replication failure on DC-DR

Identifier	Headline
CSCwp07313	Cisco SD-WAN Manager is not showing any license with the message "There are no licenses available in your license repository for the selected devices.Please add licenses or use a different Smart Account and Virtual Account with available licenses."
CSCwo49878	Cisco SD-WAN Manager count update on c8200-1N-4T triggers vdaemon high and show sdwan commands get stuck
CSCwn49053	Replication breaks for the whole cycle due to disaster recovery leadership changing during export.
CSCwn90550	SaaS/vQoE score page doesn't work without settings feature read
CSCwn82525	Cisco SD-WAN Manager GUI memory utilization discrepancy for monitor versus system status
CSCwm12022	Need retries for disaster recovery nodes to inform data center about successful replications
CSCwp14369	Catalyst Manager SSO does not parse SAML Metadata due to unsupported SOAP
CSCwm65800	dbgd should be non-critical/restartable process
CSCwn19880	Stats files are not being processed in two standby nodes
CSCwn55211	Need encryption support for SNMP SHA-256 config done using CLI add-on template
CSCwp03947	The DC (primary) cluster does not log out the replication user after config-db/stats sync by DR (secondary) cluster
CSCwp32858	Catalyst Manager SSO - EntityID/Issuer is not parsed correctly from SAML Response
CSCwo41233	Cisco SD-WAN Manager memory leak with SLA Violation events due to NWPI Auto-On Task running in the background
CSCwn78261	Cisco Catalyst 8000V certificate install failed
CSCwo72463	Template pull model creates HTTP session to Cisco SD-WAN Manager. Session is not closed properly by device
CSCwo25668	Handling device migration flow in DDC
CSCwn81861	Configuration Group: CSV File Import Error for Subnet Mask
CSCwn94652	64GB Cisco SD-WAN Manager neo4j off-heap memory keeps increasing caused oom-killer
CSCwm52650	Configuration group can not be pushed due to error Duplicate Tag Name
CSCwe66021	Enhancement - "Certificate Expiring" Alarm not present on Alarm notification.
CSCwo91297	In 20.9.5.2-li Cisco SD-WAN Manager, seeing incorrect SIM status in Monitor dashboard
CSCwj49155	DNS Channel uses same source port in every connection

Identifier	Headline
CSCwn06651	Policy Group Service Chain Errors
CSCwq21370	20.15 // IR8340 - "Device is not categorised for Licensing"
CSCwo70700	In 20.12.4 Cisco SD-WAN Manager, the rootfs.rw was filled 100%
CSCwo87819	In 20.9 code, cluster config node credentials are double encrypted
CSCwo95936	Cisco SD-WAN Manager TCP Optimization Policy Group - NullPointerException
CSCwn30415	Cisco SD-WAN Manager olap-db query_log bloated - 20.15.1
CSCwp72213	Cisco SD-WAN Manager config-db upgrade failing for clusters with higher db sizes > 8 GB (20.9 to 20.12 upgrade)
CSCwn43011	QuickConnect utility in Cisco SD-WAN Manager will not accept any .csv files in Firefox
CSCwn89407	Remote users assigned to a scope are not displayed under "assigned users" on the scope page
CSCwo33761	Periodic UTD signature upgrade task created daily, due to wrong meta data info.
CSCwn45352	UX2.0 can't deploy Policy Group, UTD VPG0 has Bad Mask /24 for address 192.1.0.255
CSCwo00098	neo4j database running out of threads after switchover
CSCwo61632	Add REST API to toggle the adaptive statistics collection
CSCwo55067	In 20.12.3.1, customer instance didn't boot after installing the web certificate and reboot
CSCwn82246	Even after completing on-demand troubleshooting, no data is displayed in SAIE.
CSCwn72244	Post disaster recovery switchover, edge serial list has to be pushed to all controllers.
CSCwo07182	Cisco SD-WAN Manager not sorting enterprise cert serial numbers by expiration date
CSCwo69197	17.12.4b Cisco IOS XE Catalyst SD-WAN device missing line config after deploying CG from 20.15.2
CSCwo31558	In multitenant environment tunnel endpoints names are displayed incorrectly
CSCwo38793	Post 20.12.4 upgrade, a remote user with namelen > 32 characters cannot access vshell
CSCwn45328	Unable to create unified policy with IPv6 rule when any other rule has AIP with TLS action decrypt
CSCwo60110	In Cisco Catalyst SD-WAN Control Components Release 20.12.4, replication is stuck in "ImportPending" on the standby cluster
CSCwo08214	Cisco SD-WAN Manager crash with error software initiated - vdaemon-4 exited with 1.

Identifier	Headline
CSCwo24776	NWPI trace does not provide the valid enduser name and ip address in Cisco SD-WAN Manager audit log

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.4

Identifier	Headline
CSCwp11066	Cisco SD-WAN Manager reloads due to ConfD got signal 9 due to clickhouse memory exhaustion
CSCwq21361	Cisco SD-WAN Manager GUI upgrade from 20.15.2 to 20.15.3 fails, user should use CLI to upgrade
CSCwm07390	In a scenario, On SNs, certificate status shows "Not Configured", even though it is configured.
CSCwm35064	High CPU utilization on multiple Cisco SD-WAN Manager cluster nodes randomly 20.9.5.2.7
CSCwi53711	[Tail-f PS-47138] Cisco SD-WAN Controller upgrade from 20.9.4.1-li to 20.12.2-li fails because of CDB boot error
CSCwq11939	OMP Site Down alarms not clearing in timely manner
CSCwe74374	TSN:C1131-8PWB - Current running config is not getting pulled for CLI template push verification
CSCwi55725	SDR CLI config group issue
CSCwn69868	Unable to come up control connections with Cisco SD-WAN Controllers after they are added and down/up
CSCwp98827	Embedded Security Rules fail to load due to high number of service profiles
CSCwj13394	Cisco SD-WAN Manager active user session gets flushed out within 10 minutes of login. This causes abrupt UI logouts
CSCwp97237	20.12.4.1 - One IDP enabled and one IDP disabled causes Internal Server Error
CSCvr12395	Cisco SD-WAN Manager push "media-type rj45" when trying to configure duplex on ISR1k
CSCwp65998	Rate limit value for URL non bulk api will be reset to default "100" after reboot in 20.12 / 20.15
CSCwm95566	Unable to activate SD-AVC Cloud Connection due to authorization failure
CSCwn69650	Follow up on lodash upgrade
CSCwn25710	API random return code 409 when switching tenants to collect data

Identifier	Headline
CSCwm26607	Cisco SD-WAN Manager 20.12 removes NAT egress-interface option from Cisco IOS XE Catalyst SD-WAN device config
CSCwp99414	Post disaster recovery switchover, certificate workflow was not able to reach to Cisco Catalyst SD-WAN Validator
CSCwk20843	PPPoE with NAT DIA feature validation failed post controller upgrade from 20.9, 20.10 to 20.12.3.1

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.3.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.3.1

Identifier	Headline
CSCwn87587	Cisco SD-WAN Manager: Java "Too many open files" error seens to due "analytics.sdwan.cisco.com" connections not being closed.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.3

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.3

Identifier	Headline
CSCwn94526	Cisco SD-WAN Manager: Error while configuring BGP comminity via configuration group
CSCwn26708	Cisco SD-WAN Manager : The Redirect DNS UX2.0 policy-group action results in a JSON Payload error.
CSCwo04528	20.15: The network hierarchy does not allow the removal of an empty subregion.
CSCwm91051	20.15.1-390- Object tracker elements are not visible in VRRP after configuring.
CSCwo19515	TACACS users are unable to login to Cisco SD-WAN Manager via GUI or CLI after Cisco SD-WAN Manager upgrade to 20.12.x
CSCwn23058	NULL entries seen on standby cluster nodes credential after standby cluster reboot/failure.
CSCwk55096	The Policy Group default application policy does not adhere to Cisco Validated Design DSCP marking.
CSCwo75184	Cisco SD-WAN Manager Sync smart or serial upload is failing due to huge neo4j query getting invoked.
CSCwn93437	Cisco SD-WAN Manager : License assignment fails with an error when the SA name contains UTF-8 characters (e.g., ร).

Identifier	Headline
CSCwo77826	20.15 // CSV file will be downloaded with empty fields (corrupted) if any template variable have "#" in it.
CSCwn59867	Cisco SD-WAN Manager 20.15.1: Cloud on Ramp for Multicloud - Failed to associate AWS account using IAM Role.
CSCwo25708	BFD_TLOC_DOWN is not distributed across all nodes in a 6 node cluster.
CSCwo07211	20.15 Can't remove optional parameter of subregion from a configuration group.
CSCwn60644	The new NGFW name is not reflected on device configuration.
CSCwk24744	Follow up on CSCwj39594. 6-Node cluster DR Replication not working in certain scenarios.
CSCwm61578	Configuration Group: Side by side preview has a scrollbar for old and new configurations.
CSCwm97346	When duplicating a CG/Profile, the old name appears at the top but cannot be selected.
CSCwo60906	Cisco SD-WAN Validator is unavailable after upgrade to version 20.15.2
CSCwn85717	SSH remains allowed even with no allow-service sshd.
CSCwm28917	Not able to update VPN Interface Cellular Feature template.
CSCwn83201	20.9.6 Cisco SD-WAN Manager keys are getting corrupted which is causing DR to break.
CSCwn06875	Configuration Group: Maximum IP MTU value for HundredGigE sub-Interface is 2000.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.3

Identifier	Headline
CSCwi53711	[Tail-f PS-46733] Cisco SD-WAN Controller upgrade from 20.9.4.1-li to 20.12.2-li fails because of CDB boot error.
CSCwn45352	UX2.0 can't deploy Policy Group, UTD VPG0 has Bad Mask /24 for address 192.1.0.255
CSCwj13394	Cisco SD-WAN Manager active user session gets flushed out within 10 min of login causing abrupt UI logouts.
CSCwm26607	Cisco SD-WAN Manager 20.12 removes NAT egress-interface option from Cisco IOS XE Catalyst SD-WAN device configuration.
CSCvr12395	Cisco SD-WAN Manager pushes "media-type rj45" when trying to configure duplex on ISR1k.
CSCwn40817	Getting intermittent error : "None of the devices belong to resource group".

Identifier	Headline
CSCwo41233	Rogue NWPI Auto-On task causing memory leak resulting in java OOM errors, causes GUI failure.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.2

Identifier	Headline
CSCwk09812	Cisco SD-WAN Manager upgrade to version 20.12.3 with 32vCPU on-prem High CPU alarms.
CSCwm51140	20.15.2: "adminresetrequired?component=configdb" API timing out on Cisco SD-WAN Manager UI.
CSCwk99406	20.15 Magnetic: After deploying mobility configuration group - WIFI parcel is missing default values.
CSCwn51103	20.15: Unable to enter comma separated subnets for IP Subnet Pool in global settings.
CSCwm84084	Web server certificate migration failure to vault after upgrade.
CSCwi69572	High CPU alarms/ alerts are seen every 30 mins to one hour in 20.6.5.1.13 code.
CSCwm30671	Creation of global setting and CGW fails when PAYG option is selected.
CSCwf98797	Summary page of nfv CG workflows shows value of "color" for the field that is labeled as "Type".
CSCwm81635	CiscoHosted: Upon upgrade to 20.12.4, sdavc custom apps are not pushed to sdavcSaas.
CSCwm94648	Color Group getting removed after Applying the AAR Policy to COR for SAAS.
CSCwm47780	Cisco SD-WAN Manager Rejects SAML Responses that Include Line Breaks.
CSCwk59590	20.15: Security Policy page loading continuously for read only users with custom scope.
CSCwh55434	Elasticsearch server CPU high due to JVM JIT deoptimization issue on getMonthOfYear().
CSCwf90168	False error "Subject serial num mistmatch" come up on ZTP server syslog.
CSCwm39910	Cisco SD-WAN Manager : License count mismatch between Cisco SD-WAN Manager & CSSM portal with Online reporting.
CSCwm26568	Cisco SD-WAN Manager DR : Replication not happening due to Lock not released on Standby.
CSCwk98041	With one interconnect connection VPN update, other interconnect connections VPN gets updated in ICGW.

Identifier	Headline
CSCwk87125	Bfd events are not getting published to messaging server in cluster setup.
CSCwm01262	Failure to deploy same NFV CG with Switch parcel to different NFVIS devices. Validation error on switch.
CSCwc04678	The data-policy-commit-failure notification promote to alarm.
CSCwm72803	Cisco SD-WAN Manager DR: DR registration doesnt proceed and task is stuck for 12+ hours.
CSCwm08353	WANI app lists are shown in policy compliance check.
CSCwi72623	Change partition task stuck, during Cisco SD-WAN Manager upgrade activation from 20.12 to 20.14
CSCwn18454	Configuration Group: cannot Save IPSEC Feature after edit.
CSCwm69595	Cisco SD-WAN Manager UI menu doesn't reflect the Configuration -> Devices post cluster upgrade to 20.12.x.
CSCwm29196	Site selected in topology policy are not saved.
CSCwk79993	[MRF] Region field is missing from the internal parcel while deploying the config-group.
CSCwk67930	Cisco SD-WAN Manager GUI becomes intermittently unavailable on 20.9.3 cluster in round robin fashion
CSCwk66060	OMP extranet policy not exporting all the routes for the prefixes.
CSCwm43112	In Cisco SD-WAN Manager running 20.12.1 code, the DE registration was stuck in pending state for several days.
CSCwm97132	Import configuration group task fails with TACACs server configuration present.
CSCwn30334	Cannot add transport to Multi Region Fabric.
CSCwk66686	Cisco SD-WAN Manager NMS services do not start after upgrading from 20.9.3ES2 to 20.15EFT2
CSCwk74774	Local User not able to login on Cisco SD-WAN Manager 20.12.3, auth-fall back fails when "priority" is configured.
CSCwm07209	Custom logo does not work on Cisco SD-WAN Manager.
CSCwm13281	Introduce Transaction timeout in Neo4j.
CSCwm63423	Route policy template: Statements missing from deployed route-map.
CSCwj17284	The communication between Cisco SD-WAN Managercluster gets break due to routes overlapping with Eth4 interface.
CSCwj29915	Preferred color group not available in traffic policy.

Identifier	Headline
CSCwn34135	DCA folder grows, the volume size of /opt/data is affected.
CSCwi43016	Need pop-up to display warning banner on 20.9 and 20.12 stating "SHA/AES-128 deprecation" .
CSCwm91228	MTT : Tenant creation fails "Failed to create tenant".
CSCwm79728	Configuration group deployment: Device variables not grouped together.
CSCwm11848	Cisco SD-WAN Manager VPN templates corrupted after upgrade to 20.12.x.
CSCwm45532	DR switchover: BFD tloc down alarms are not getting cleared thereby causing stale alarm issues.
CSCwi21976	Cisco SD-WAN Manager API: User with only Interface read-only access can see the connected user list.
CSCwm72199	The 'service local' is not pushed to WAN Edges after upgrade from 20.9.5 to 20.12.4.
CSCwi85554	Cisco SD-WAN Manager cannot deploy a configuration group on a Cisco IOS XE Catalyst SD-WAN device added by a tag rule.
CSCwk92103	Cisco NFVIS SD-Branch: 2nd device not upgrade in the same site-id after the 1st device is upgraded successfully
CSCwk55953	Policy Group: Cloud OnRamp gateway service VPN is only showing VPN 512 interfaces.
CSCwi99563	Unable to edit object tracker on static NAT entries when there are a lot of entries.
CSCwm07628	Not able to add new tracker while using Generic on Cisco Secure Internet Gateway (SIG).
CSCwm42868	Cisco SD-WAN Manager upload NBAR Protocol Pack fails.
CSCwm70614	Statistics data is not visible after upgrading to 20.12.3.1 MTT setup.
CSCwm09327	Wasted space in Policy Application page.
CSCwm52596	Network Hierarchy should not have white spaces, unable to activate topology group.
CSCwk93952	SDWAN-Manager : DR Replication failure due to thread's getting stuck.
CSCwk48991	Transport Gateway: WAN Edge Receives Re-Originated Route with it's own Site ID.
CSCwi95474	6 + 6 DR cluster elects replication leader which has no config-db and fails to connect to Neo4j.
CSCwk89814	20.15 - Cisco SD-WAN Manager generates UTD container profile as low though profile is configured as high/medium !
CSCwm54703	20.9.4.1 Cisco SD-WAN Manager app-server restarted due to app-server OOM Java heap space.

Identifier	Headline
CSCwk61793	After Applying SaaS, AAR Policy in the GUI differs from AAR Policy in the CLI.
CSCwm88561	Cisco SD-WAN Manager single node upgrade: upgrade coordinator task is stuck.
CSCwm74318	Configuration group: Switchport parcel interface errors and variables are cut off by window size.
CSCwm01992	Save option greyed out when trying to edit SNMP parcel.
CSCwm60082	CloudOps unable to leverage ciscotacrw for maintenance when DUO is configured.
CSCwm72404	Host-agent Failed to activate MT DR single node Cisco SD-WAN Manager Error: Software Operations script failed.
CSCwm09476	ND deployment fail Deployment c8kv failed with error: Bootstrap File not found.
CSCwj75749	Edit of basic parcel fails with "Required But Missing Attributes for transportGateway.value"
CSCwm73952	Cisco SD-WAN Manager upgrade from 20.12.3.1 to 20.15.1 fails in post-upgrade-check-fail.
CSCwm68939	Customer migrated from 20.9.5 to 20.15.1 and all their devices are showing no license assigned.
CSCwm53003	Making messaging-server robust.
CSCwn05679	TAC Case Option in Cisco SD-WAN Manager does not redirect correctly.
CSCwn10660	Importing the SDWAN CG fails due to validation errors: data.advanced.tracker is not defined in the schema attributes.
CSCwh24335	Manipulate driver of Neo4j and ES to use static logger instead of new logger (Cisco SD-WAN Manager Slowness 20.6)
CSCwm60069	Configuration group: Feature parcels from policy profile are duplicated by copy function.
CSCwm85904	SDWAN Manager: control policy is getting removed during configuration sync.
CSCwk61155	Virtual device CoR SaaS info not cleaned up from DB on decommissioning.
CSCwj71739	Viptela Platforms are not following RFC standard for command accounting.
CSCwm76848	Creation of customer policy configuration from API fails on latest 20.16
CSCwk87578	Continuous logs being generated by Cisco SD-WAN Manager.
CSCwm77677	Configuration group: Dual router feature parcel 'save' issues.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.2

Identifier	Headline
CSCwm96920	20.15.2 : UTD installation failing due to Error 416 after doing DR Switchover.
CSCwn55211	Need encryption support for SNMP SHA-256 config done via add-on CLI.
CSCwn26708	Cisco SD-WAN Manager : Redirect DNS UX2.0 policy-group action gives JSON Payload error.
CSCwm07390	In a scenario, On SNs, Certificate Status shows "Not Configured", even though it is configured.
CSCwm56572	Cisco SD-WAN Manager GUI is continuously loading and display of backend code indicating potential code leakage.
CSCwk85210	2015: CSDL GET /device/models Fails Ace tests.
CSCwj85502	Brownfield Scenario: Able to select cxp app lists in DIA and SIG.
CSCwn51488	Multiple active userSessions exist on Cisco SD-WAN Manager even after controller upgrade transaction completes
CSCwm28696	20.15:SD-routing CG parcel Deployment-status show Sync Pending - Device is offline/Re-deploy CG fix.
CSCwi53711	[Tail-f PS-46733] Cisco SD-WAN Controller upgrade from 20.9.4.1-li to 20.12.2-li fails because of CDB boot error.
CSCwn45352	UX2.0 can't deploy Policy Group, UTD VPG0 has Bad Mask /24 for address 192.1.0.255
CSCwj13394	Cisco SD-WAN Manager active user session gets flushed out within 10 min of login causing abrupt UI logouts.
CSCwe74374	TSN:C1131-8PWB - Current running configuration is not getting pulled for CLI template push verification.
CSCwn91520	SDWAN: "Routing DNA HA Advantage" license not visible in Cisco SD-WAN Manager.
CSCwm36264	IPv6 Prefix push template fails.
CSCwn25710	API random return code 409 when switching tenants to collect data.
CSCwn83201	20.9.6 Cisco SD-WAN Manager keys are getting corrupted which is causing DR to break.
CSCwn12834	Neo4j/GUI is not coming up after Virtual Machine size upgrade.
CSCwn69868	Unable to come up control connections with Controllers after Controllers added and down/up.
CSCwn30415	Cisco SD-WAN Manager olap-db query_log bloated - 20.15.1

Identifier	Headline
CSCwk06118	Import PG fails: Reason: [{"Validation Errors":{"Required But Missing Attributes"}}].
CSCwn90370	20.9.5.1 Database panic - The database has encountered a critical error.
CSCwm35064	High cpu utilization on multiple Cisco SD-WAN Manager cluster nodes randomly 20.9.5.2.7
CSCwm35108	Neo4j getting killled due to OOM resulting in GUI being unavailable even with enough resources.
CSCwn05583	Soln: 20.15.2 unable to push Cisco SD-WAN Controller configuration diff PG from Cisco SD-WAN Manager
CSCwm95566	Unable to Activate SD-AVC Cloud Connection due to Authorization Failure.
CSCwm26607	Cisco SD-WAN Manager 20.12 removes NAT egress-interface option from Cisco IOS XE Catalyst SD-WAN device configuration.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.x

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.1

Identifier	Headline
CSCwj10872	Unable to upload the file by drag and drop function.
CSCwk32515	Delayed notification (webhook) when one of the Webhook server is unreachable.
CSCwj85252	Cisco VPN Interface IPsec template does not send selected parameters to device.
CSCwk37436	Region ID assignment from Network Hierarchy is not mapped to the CLI configuration.
CSCwk14972	Cisco SD-WAN Manager : Serviceproxy hitting UpstreamOverflow-503/RateLimited-429 causing GUI down issues.
CSCwk27179	OMP: Advertiser IPv4 EIGRP cannot configured by Configuration Group.
CSCwk74660	On-prem CSSM server with IPv6 address gives Error while fetching sa/va list RESTEASY004655.
CSCwj37051	Cisco SD-WAN Manager CLI template fails to attach to CG418-E/CG522-E with error "access-denied".
CSCwj87791	POST /template/device/cli Example is not accurate - apidocs.
CSCwi90351	Uuid in certificate CN checks are case-sensitive, request for uuid checks to be case-insensitive.
CSCwj06854	Cisco IOS XE Catalyst SD-WAN Release 17.14.x UX1.0 Config preview show partial output for Static NAT configuration (interface missing).

Identifier	Headline
CSCwj38614	Cisco Catalyst SD-WAN Manager Release 20.13.x: Enforce software version (ZTP) selected version is not reflected after save.
CSCwk35796	Cisco SD-WAN Manager RealTime show commands display incorrect time when devices are configured with IST timezone.
CSCwi31443	Cisco vEdge device cannot resolve Cisco SD-WAN Validator after reboot for software activation.
CSCwj77440	Cisco SD-WAN Manager apidocs missing schema for some parcels.
CSCwj81863	The rest API uniqueAggregation and cellularAggregation need enahnce example and schema.
CSCwi52276	System crash rebooted with "Software initiated - zebra-1 (pid: 4221)"
CSCwk30596	Cisco SD-WAN Manager: Smart account sync API timeout increase.
CSCwj58673	Cisco Catalyst SD-WAN Manager Release 20.14.x : 206 to 231 build. DR : Standby cluster. services One of the node do not start.
CSCwk39051	Validation Error when using public-internet or red color in custom topology policy.
CSCwk61142	Cisco SD-WAN Manager email alarms failing with SSL and TLS connecting to incorrect port 465.
CSCwk88478	VRRP default timer shows 1000ms in GUI but it show 100ms in preview and pushed 100ms to device.
CSCwi69833	Cisco SD-WAN Manager GUI SSH frontend sends too many requests to backend leading to timeouts, session closed.
CSCwk50045	Cisco SD-WAN Manager - ZTP doesn't permit to select a software.
CSCwj99812	Creating a new branch site on Cisco SD-WAN Manager network design using an old name is failing.
CSCwi87770	Custom rollback timer does not take effect.
CSCwj84723	Harden Cisco SD-WAN Manager certificate process.
CSCwj53683	Cisco SD-WAN Manager variables inconsistent for CSV export of device template.
CSCwk23323	Cisco SD-WAN Manager Cluster: When device is deleted from UI, the NCS entry does not get cleared on all nodes
CSCwj76609	Cisco SD-WAN Manager: Unexpected Reload when Modifying DNS Server Configuration
CSCwj57249	For event based alarms-missing event from device breaks Alarm logic-ReferCSCwj21640 Cisco SD-WAN Manager side fix.

Identifier	Headline
CSCwk37757	Interface API Fails to Fetch Duplex State for Cisco IOS XE Catalyst SD-WAN device interfaces.
CSCwk22840	In 20.9.5.1, deleting the Disaster Recovery is not cleaning the database and the files.
CSCwj69758	On-Demand Tunnel is reported as down on Cisco SD-WAN Manager GUI for several hours.
CSCwk31416	Integration Management page in UI can't populate device list intermittently : rendering issue.
CSCwk27624	Control Policy is Programmed Incorrectly on Cisco SD-WAN Controller.
CSCwj89979	FIS - GUI UX Slowness - CSCwh28301.
CSCwk24904	CG522 - Data connection fails after a sim switchover.
CSCwk19371	Cisco SD-WAN Manager: Netconf errors and slow login.
CSCwc67155	Cisco SD-WAN Manager : HTTP proxy not using ICMP echo requests.
CSCwk00758	Feature name description does not match feature name auto generated from color selected.
CSCwj89565	Template pushes are taking a lot of time for scale setup.
CSCwj87100	Cisco SD-WAN Manager : Looses the entity-ownership after upgrade.
CSCwi59683	MT Controllers - show control connection history doesn't list org name.
CSCwk70854	Evaluation of Cisco SD-WAN Validator for BlastRADIUS vulnerability.
CSCwk70903	BlastRADIUS - RADIUS Protocol impact - CVE-2024-3596.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.15.1

Identifier	Headline
CSCwm09317	Incorrect site deleted from sorted list Configuration > Policies > Edit Policy > Policy Application.
CSCwq91481	DR: Scale configuration causes neo4j to crash and restart in secondary when deleting & importing SYSTEMDEVICESNODE.
CSCwk09812	Cisco SD-WAN Manager upgrade to version 20.12.3 with 32vCPU on-prem High CPU alarms.
CSCwm08353	WANI App lists are shown in policy compliance check.
CSCwm09265	Server names - Asterisk is not required for custom applications.
CSCwk41441	Cisco SD-WAN Manager template push failed config pull with "Failed to finish the task".

Identifier	Headline
CSCwk85198	Cisco SD-WAN Manager 20.15.1: MC MRF: Audit Out-of-sync and Unmapping failed.
CSCwk23821	Cisco SD-WAN Manager 20.13.1 last-resort circuit button is not doing effect in configuration group.
CSCwk66060	OMP extranet policy not exporting all the routes for the prefixes.
CSCwk79499	Variable field is missing for second UCS-E blade while pushing the template.
CSCwm09327	Wasted space in Policy Application page.
CSCwk66113	"Change Device Values" option removed in Cisco SD-WAN Manager 20.15.
CSCwk37657	The devices brought up with PNP when pre deployed to a config group do not receive the full configuration.
CSCwk74774	Local User not able to login on Cisco SD-WAN Manager 20.12.3.
CSCwk87125	Bfd events are not getting published to messaging server in cluster setup.
CSCwk60384	Controller establishes multiple viptela-device session and affects performance.
CSCwj71739	Viptela Platforms are not following RFC standard for command accounting.
CSCwm01262	Fail to deploy same NFV CG with Switch parcel to different NFVIS devices. Validation Error on Switch.
CSCwm01992	Save option greyed out when trying to edit snmp parcel.
CSCwk89814	Cisco SD-WAN Manager 20.15 - Cisco SD-WAN Manager generates UTD container profile as low though profile is configured as high/medium !
CSCwm59794	Default values for variables name in configuration group aren't accepting more than 60 characters.
CSCwq33835	DR replication fails with large configuration - Neo4j OOM on standby
CSCwp05800	[20.12] Drop labels/nodes cause OOM on scaled setup

Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations.

Cisco Catalyst SD-WAN Manager API

For information on Cisco SD-WAN Manager Release 20.15.x APIs, see Cisco SD-WAN Manager API.

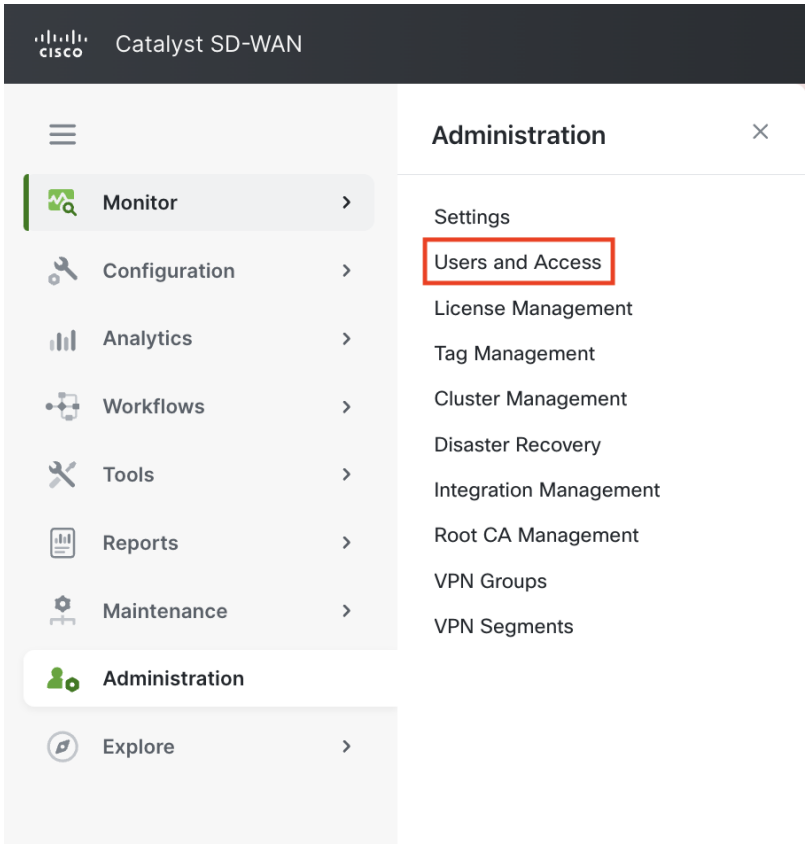
Cisco Catalyst SD-WAN Manager GUI Changes

This section presents a summary of the significant GUI changes between Cisco Catalyst SD-WAN Manager Release 20.14.1 and Cisco Catalyst SD-WAN Manager Release 20.15.1.

- Administration menu, Users and Access

  In the **Administration** menu, the **Manage Users** menu is renamed to **Users and Access**.

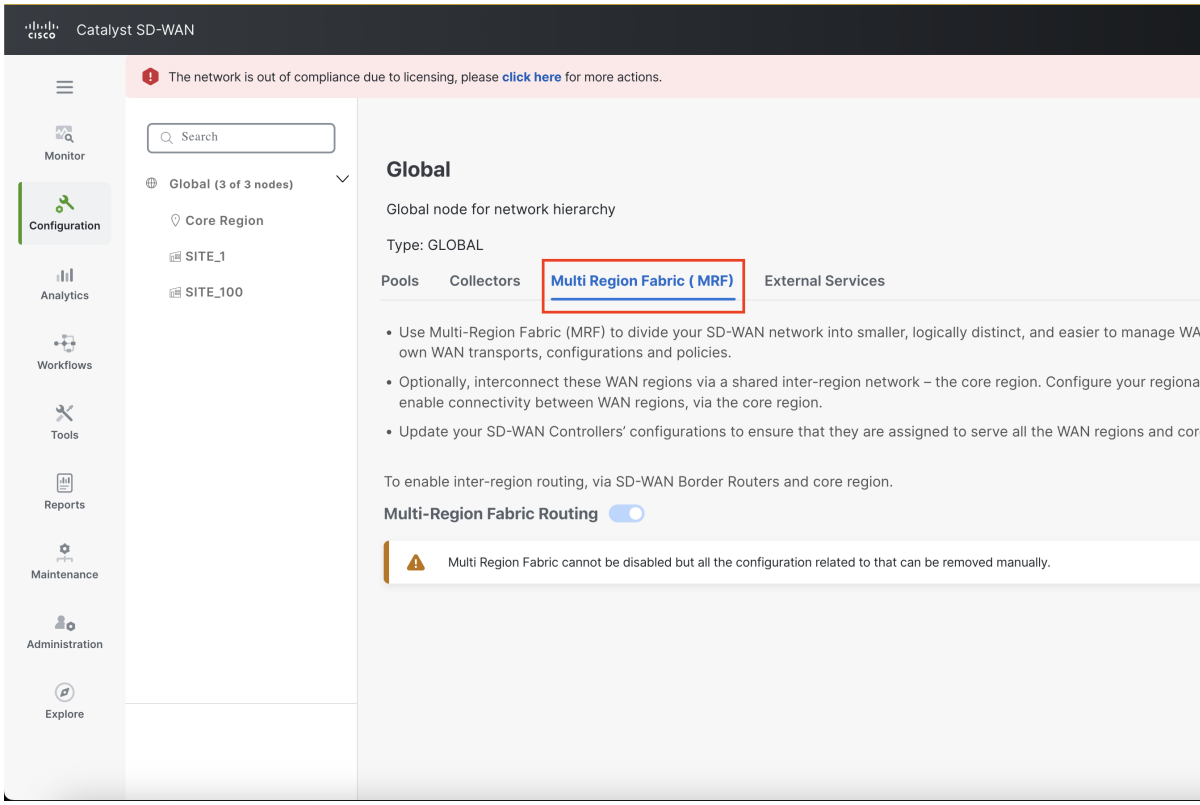
  Figure 1: Administration Menu



- Network Hierarchy page, Multi Region Fabric (MRF) tab

  On the **Configuration** > **Network Hierarchy** page, the **Network Settings** tab is renamed to **Multi Region Fabric (MRF)**.

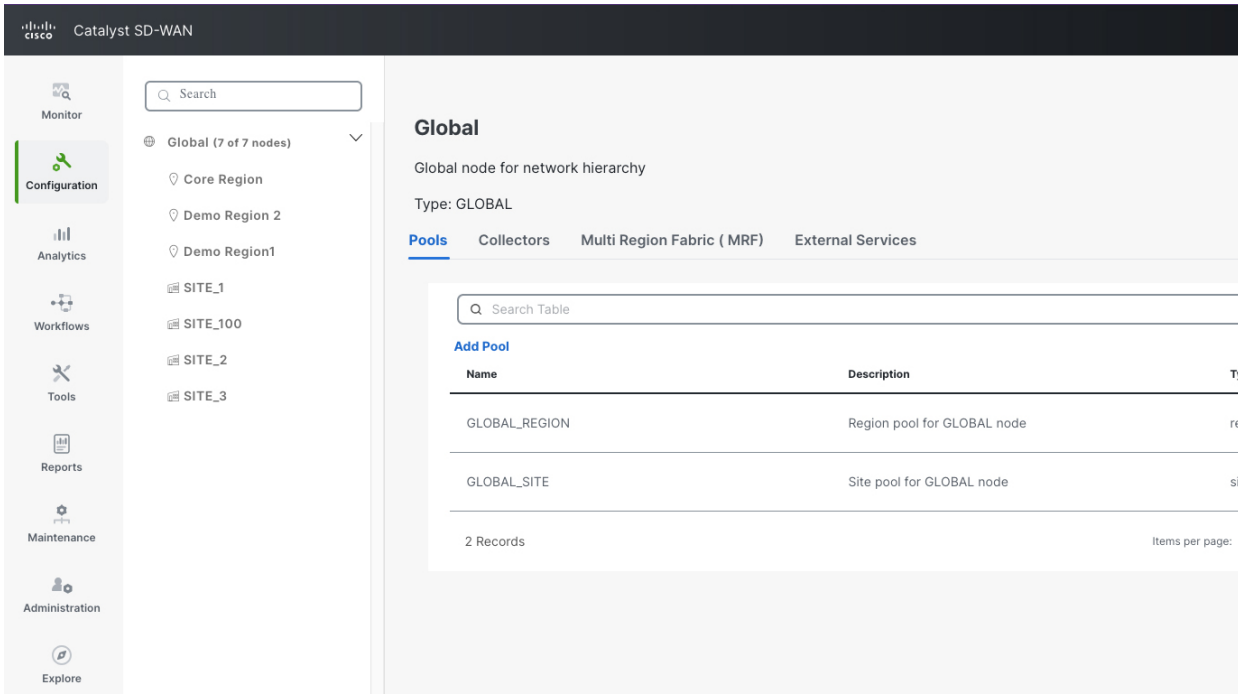
Figure 2: Network Hierarchy Page, Multi Region Fabric (MRF) Tab



- Secondary regions and subregions

  On the **Configuration** > **Network Hierarchy** page, it is no longer possible to create secondary regions or subregions. From this release, these are supported only through API.

Figure 3: Network Hierarchy Page



AI Assistant on Cisco SD-WAN Manager

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1

On Cisco SD-WAN Manager, click Cisco AI Assistant. The AI assistant is available only to cloud customers. You can use this feature for the following use cases:

- Product and Features: Provides information about Cisco Catalyst SD-WAN and the features introduced in this release.
- Monitor Network: Provides information about the network and application health.

To enable the AI assistant feature:

1. Enable cloud services in **Administration** > **Settings**.
2. Enter the **Smart Account Credentials** and click **Save**.

Related Documentation

- Release Notes for Previous Releases
- Software Installation and Upgrade for vEdge Routers
- Field Notices
- Recommended Releases
- Security Advisories

- Cisco Bulletins
- Cisco Recommended Catalyst SD-WAN Software Versions for Controllers and WAN Edge Routers

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024–2026 Cisco Systems, Inc. All rights reserved.